

COMMUNICATIONS TECHNOLOGY INTERNET OF THINGS IN CISCO PACKET TRACER

Pavel Beneš

Master Degree Programme (2), FEEC BUT

E-mail: xbenes48@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak

E-mail: fujdiak@feec.vutbr.cz

Abstract: This work is aimed at simulating the Internet of Things in Packet Tracer. In this work, a network containing IoT devices is created in the Packet Tracer simulation program. In the network, the parameters affecting the quality of the network are subsequently monitored, depending on the number of connected devices, and these measured values are subsequently evaluated.

Keywords: Delay, Internet of Things, Packet Loss, Packet Tracer

1 ÚVOD

Internet věcí je v dnešní době velice diskutovanou technologií a v budoucnosti bude ještě více kvůli širokým možnostem nasazení. Využití má především ve zdravotnictví, průmyslu, v dopravě a ve městech. S tím souvisí převážně komunikace stroj - stroj, kdy probíhá komunikace převážně mezi zařízeními bez nutnosti zásahu člověka. Slouží k řízení pracovních procesů, sběru, analýze a vyhodnocování dat. Nesmí být ani opomenuta komunikace typu člověk - stroj, stroj - člověk a člověk - člověk. Komunikace v poslední době probíhá hlavně pomocí nízkovýkonových zařízení, a tím roste nutnost nasazování nových komunikačních protokolů a technologií.

Packet Tracer je simulační prostředí pro výukové účely Cisco Networking Academy. Packet Tracer je pro studenty volně ke stažení. Je to multiplatformní aplikace, která pracuje jak pod OS Windows, tak pod OS Linux. Aktuálně vydaná verze je 7.1. Tato simulace má za úkol zjistit, jak se bude chovat navrhované prostředí v reálném nasazení. Je tedy nutné vytvořit síť s prvky Internetu věcí a především analyzovat všechny části a prvky sítě a použít nejvhodnějších z nich. Následně provést měření doby odezvy a ztrátovosti paketů.

IoT (Internet věcí - Internet of Things) je rychle se rozvíjející oblastí informačních technologií, která slouží ke komunikaci a kontrole předmětů, které jsou využívány v běžném životě. Zařízení mezi sebou mohou být propojeny pomocí internetu, ale nemusí tomu být jenom tak, stačí když zařízení budou propojeny do jakékoliv lokální sítě, ve které spolu budou moci komunikovat. Jako věc je v tomto případě brán jakýkoliv neživý objekt, jak fyzický, tak virtuální, který obsahuje elektroniku, software a senzory, pomocí kterých sbírá potřebné informace, které následně vyhodnocuje a sdílí s ostatními věcmi v síti. Ty poté podle potřebných dat mohou vykonávat určitou aktivitu. To pro nás znamená, že čím více bude zařízení, tím více bude poskytnutých dat o reálném světě, tím budeme mít více dat k vyhodnocení a tím více znalostí bude možné aplikovat. Hlavními požadavky na IoT jsou: sběr dat/informací/znalostí, uložení dat/informací/znalostí, analýza dat/informací/znalostí, sdílení výsledků, bezpečnost [1, 2].

2 TESTOVACÍ PROSTŘEDÍ

Testování probíhalo ve virtuálním prostředí programu Packet Tracer 7.1.0.0222, do kterého bylo vložena dvě zařízení DLC 100, které nám sloužily pro projení IoT zařízení a jejich možné komunikaci.

DLC 100 byly přiděleny IP adresy 192.168.25.1 a 192.168.26.1 s maskou 24 bitů pro lokální síť a IP adresy 185.21.220.1 a 185.21.220.2 s maskou 24 bitů pro síť sloužící k propojení.

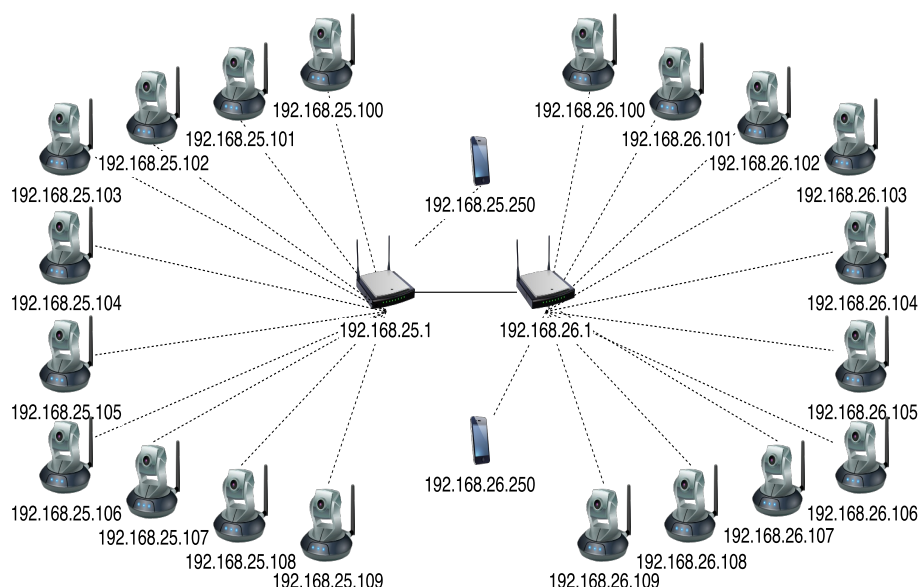
Dále byly do prostředí vkládány prvky IoT které byly připojeny do Wi-Fi sítě s názvem HomeGateway1 a HomeGateway2 vytvořené na zařízeních DLC 100. Zařízení měly IP adresy z rozsahu 192.168.25.2 - 192.168.25.241 s maskou 24 bitů pro HomeGateway1 a IP adresy z rozsahu 192.168.26.2 - 192.168.26.241 s maskou 24 bitů pro HomeGateway2.

Měření probíhalo pomocí příkazu ping, který měl tvar:

```
ping -n 20000 192.168.25.x
```

kde x byla adresa IoT zařízení. Parametr -n nám zaručuje odeslání 20000 ICMP zpráv, který nám zaručoval dostatečný počet zpráv k vyhodnocení výsledků.

Testování probíhalo nejdříve dotazováním na 2 IoT zařízení a konec měření byl na 24 IoT zařízení, proběhlo 12 měření. Současně navíc každé zařízení v intervalu 0.3 sekundy posílalo zprávu o velikosti 2048 kB, tato velikost odpovídá zhruba jednomu snímku v rozlišení 3840 x 2160 pixelů a tento čas nám dává přehledové denní o monitorovaném prostoru. Pro první měření v každé síti bylo připojeno 10 IoT zařízení a jeden mobilní telefon, na každé další měření byl nárůst o 10 zařízení a jeden mobilní telefon. Schéma zapojení pro první měření je na Obr. 1.



Obrázek 1: Schéma úvodního testovacího prostředí v programu Packet Tracer.

3 EXPERIMENTÁLNÍ MĚŘENÍ DOBY ODEZVY A ZTRÁTOVOSTI

Doba odezvy je časový úsek, který udává, za jak dlouho dorazí odpověď na dotaz jiného zařízení. Z naměřených hodnot, kdy při pravidelném dotazování příkazem ping a narůstajícím zatížením sítě byly vypočítány průměrné hodnoty na každé měření. Na Obr. 2 je vidět, jak s větším počtem připojených zařízení a tedy i se zvyšujícím se zatížením sítě, roste doba odezvy. Měření nám nesaturovalo z důvodu, že síť na které probíhalo měření nebyla plně vytížena. Pokud bychom pokračovali v měření dál, vzrostla by odezva tak, že by zařízení DLC 100, začalo pakety zahazovat a tím by nám přestala růst doba odezvy a pro další měření by nám zůstala konstantní.

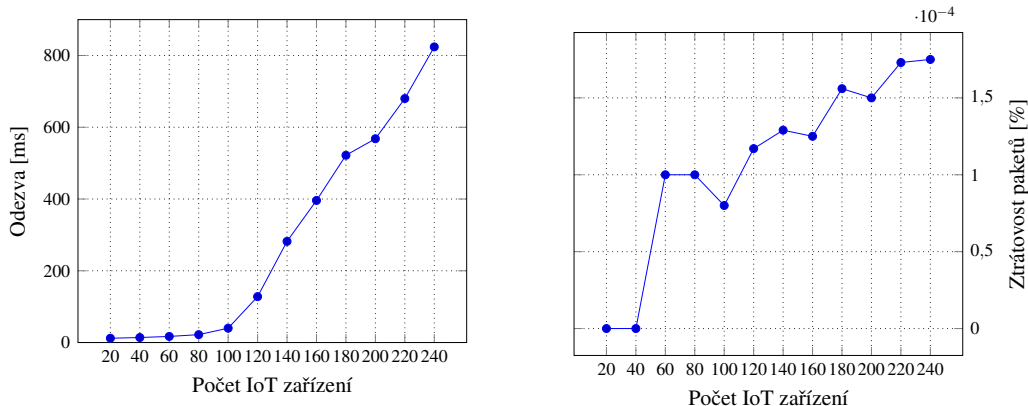
Ztrátovost chyba při které se ztratí jeden nebo více paketů v počítačové síti. Ztrátu paketů může způsobit více okolností. Největší vliv mají ty vlastnosti: zhoršená kvalita signálu, zahazení paketu z dů-

vodu zahlčení sítě, poškozené pakety zamítnuté během přenosu, selhání síťového hardwaru, selhání síťových ovladačů, nebo běžného směrování. Procentuální rovnice ztrátovosti je:

$$LR = \frac{P_a}{P_s} \cdot 100 [\%], \quad (1)$$

P_a = udává počet přijatých paketů a P_s = udává počet odeslaných paketů.

Z naměřených hodnot, kdy při pravidelném dotazování příkazem ping a narůstajícím zatížení sítě byly vypočítány průměrné hodnoty na každé měření. Na Obr. 3 je vidět, jak při nižším počtu připojených zařízení je ztrátovost nulová, s rostoucím počtem zařízení následně roste i počet ztracených paketů v síti. Ztrátovost je velmi nízká, při testování nebylo ztraceno víc jak 0.002% paketů na měření. Ztrátovost byla nízká z důvodu, že síť na které probíhalo měření nebyla plně vytížena. Pokud bychom pokračovali v měření dál, vzrostla by odezva tak, že by zařízení DLC 100, začalo pakety zahazovat a tím by nám začala růst ztrátovost paketů.



Obrázek 2: Doba odezvy v závislosti na počtu IoT zařízení. **Obrázek 3:** Ztrátovost paketů v procentech na počtu IoT zařízení.

4 ZÁVĚR

Z naměřených hodnot, kdy při pravidelném dotazování příkazem ping a narůstajícím zatížení sítě byly vypočítány průměrné hodnoty ztrátovosti paketů a doby odezvy. Z naměřených hodnot jde usoudit, že zvolený provoz sítě zatížil pouze z hlediska doby odezvy. Ztrátovost paketů byla minimální a nepřesáhla 0,002% paketů na měření. Tyto nízké hodnoty se dají přisoudit tomu, že síť nesaturovala při měření doby odezvy a tedy nebyla plně zatížena.

REFERENCE

- [1] AL-FUQAHA, Ala, Mohsen GUIZANI, Mehdi MOHAMMADI, Mohammed ALEDHARI a Moussa AYYASH. *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications* [online]. 2015, 2347-2376 [cit. 2018-03-10]. DOI: 10.1109/COMST.2015.2444095. ISSN 1553-877X.
- [2] Security Requirements Analysis for the IoT. *2017 International Conference on Platform Technology and Service (PlatCon)* [online]. IEEE, 2017, 1-6 [cit. 2018-03-08]. DOI: 10.1109/PlatCon.2017.7883727. ISBN 978-1-5090-5140-3.